TRANSLATION

of DE 195 21 902 A1 (SEL ALCATEL AG)
Col. 1, line 64 to Col. 5, line 50

...

In the following the invention is explained by way of two embodiments and with the aid of Figs. 1 to 5:

Fig. 1 shows a schematic representation of a first embodiment of the inventive security system for motor vehicles,

Fig. 2 shows a schematic diagram of an inventive security device for the security system of Fig. 1,

Fig. 3 is a schematic representation of a control unit for the inventive security device of Fig. 2,

Fig. 4 is a schematic diagram of an inventive control centre for the security system of Fig. 1, and

Fig. 5 is a schematic representation of a second embodiment of the inventive security system for motor vehicles.

A first embodiment of the invention is now described in accordance with Figs. 1 to 4.

Fig. 1 shows a first embodiment of an inventive security system SYS comprising a radio system FS, a motor vehicle KFZ and an ignition key ZS. The security system SYS serves for protecting motor vehicles KFZ against unallowed use from a control centre ZE via radio signals. For the sake of explaining the invention, only the securing of one motor vehicle in one radio cell of the radio system FS is described. The same applies to securing several motor vehicles in several radio cells.

The motor vehicle KFZ, e.g. passenger car or motor lorry, contains a security system SE with an antenna through which the security system SE can communicate with the control centre ZE. The antenna is for example an antenna of a GSM-mobile station, which may be contained in the security device.

The radio system FS is configured as a cellular mobile radio system according to GSM-standard; GSM stands for Global System for Mobile Communication. Such a cellular mobile radio system is for example known

from the book "The GSM System for Mobile Communications", 1992, M.Mouly and M. Pautet, Int. Standard Book Number 2-9507190-0-7, pages 94 to 98 and 309 to 312. The radio system FS comprises a fixed radio station BTS, a fixed radio station control BSC, a radio exchange MSC and the control centre ZE. The fixed radio station BTS is connected to the control centre ZE via the fixed radio station control BSC and the radio exchange MSC.

The ignition key ZS contains an infrared-transmitting unit IRS, a counting device N and a switch S operable by touch of the finger. The infrared-transmitting unit IRS serves for transmitting infrared signals to the security device SE in the motor vehicle KFZ. The counting device N is a device for generating binary bit sequences of fixed length, wich are transmitted to the security device SE via the infrared-transmitting unit IRS and the value of which changes with each transmission. The counting device N is controlled via switch S. The count of the counting device N is increased by each actuation of the switch S by one unit and transmitted via the infrared-transmitting unit IRS.

Fig. 2 shows a schematic diagram of the security device SE of Fig. 1.

The security device SE comprises three means AN, ZD, KP which are required for starting the motor vehicle KFZ, i.e. a starter AN, an ignition coil ZD and a fuel pump KP, each with electronic control. The security device SE serves for making the three means AN, ZD, KP electronically ready for operation or to block them. For this purpose the security device SE contains a control device CTRL, an infrared-receiving unit IRE, a transmitting equipment SEN, a receiving equipment EMP and an antenna ANT. The control devic CTRL controls the three means AN, ZD, KP in response to the signals received via the infrared-receiving unit IRE and the receiving equipment EMP. For this purpose, the control device CTRL is connected with the three means AN, ZD KP, the infrared-receiving unit IRE, the transmitting equipment SEN and the receiving equipment EMP. The transmitting equipment SEN and the receiving equipment EMP are connected with the antenna ANT.

Fig. 3 shows a schematic representation of the control device CTRL of Fig. 2.

The control device CTRL comprises a computing unit RE, e.g. a microprocessor having two inputs and three outputs. The first output is connected with the ignition coil ZD, the second output with the starter AN and the third output with the fuel pump KP. The ignition coil ZD, the starter AN and the fuel pump KP are made ready for operation in response to the signals applied to the two inputs of the computing unit RE, whereby for example the voltage supply for the ignition coil ZD, the starter AN and the fuel pump KP, each, is connected via a relais. Each time the engine is switched off, ignition coil ZD, starter AN and fuel pump KP are blocked by the computing unit RE in that, for example, the voltage supply via a relais is cut off. For this purpose, for example, a control signal is transmitted from the engine control to the computing unit RE as soon as the engine is switched off. A renewed startup of the motor vehicle KFZ is only possible via new input signals for the computing unit RE. The new input signals have to differ from the input signals of the previous startup. A first input signal for the control device CTRL is derived from the infrared-signal of the igntion key ZS, a second input signal from the radio signal of the control centre ZE. If both input signals are identic, ignition coil ZD, starter AN and fuel pump KP are made ready for operation.

The control device CTRL further incorporates a comparator VER, an updating unit AKT, a memory MEMO, a read-in unit IN, a read-out unit OUT and an identification unit ID. First, the infrared signal of the ignition key ZS is supplied to the comparator VER. Inside the comparator VER a comparison between the count, contained in the infrared signal and a count stored in the updating unit AKT takes place. If the count of the infrared signals is at least by one unit and at most by ten units higher than the count of the updating unit AKT, the infrared signal is transferred and the count in the updating unit AKT is replaced by the count of the infrared signal. Having passed the comparator VER the infrared signal is supplied to the identification unit ID. Inside the identification unit ID an individual indentification number of the

motor vehicle KFZ is added to the count of the infrared signal. Both, count and identification number on the one hand serve as a first input signal for the computing unit RE and on the other hand form a request signal which is radio-transmitted via the transmitting equipment SEN of the security device SE to the centre ZE.

The centre ZE evaluates the request signal, checks if the identification number is contained in a database, and - if the identification number is in the database - transmits five encoded radio signals to the control device. The five encoded radio signals are read-in into the memory MEMO via a read-in unit IN and are stored. The first encoded radio signal contains the count of the infrared signal and the identification number in encoded form and is stored under the memory address corresponding to the count of the infrared signal. The second encoded radio signal contains the count increased by one unit and the identification number and is stored under the memory address with the value of the count increased by one unit. The same applies to the third, fourth and fifth radio signals.

The control device CTRL further contains an exclusive-OR-gate XOR, an RSA decoding unit RSA and a read-only memory KEY2, wherein a public key is stored. RSA means Rivest, Shamir, Adleman. According to RSA signals can be asymmetrically encoded and decoded. The encoding method according to RSA is for example known from the book "Chipkarten-Technologie in der Anwendung"*, 1995, pages 47 to 54, Wissenschaftsverlag Volker Spiess GmbH, Berlin, ISBN 3-89166-183-5. *[Chip card technology and application thereof].

The centre ZE encodes signals by a secret key according to the RSA-algorithm. The secret key, for example, is 512 bits long and only known to the centre ZE. For decoding in accordance with the RSA-algorithm, the control device CTRL in the motor vehicle KFZ incorporates a public key, which may be used for several motor vehicles KFZ and which may also be known to the public.

The exclusive-OR-gate XOR has two inputs and one output. The output is connected via the RSA-decoding unit RSA with the second input of the

computing unit. The count of the infrared signal is applied to the first input. The memory contents belonging to the memory address corresponding to the count of the infrared signal are applied to the second input. Thus, the contents of the memory are linked with the count of the infrared signal, supplied to the RSA-decoding unit RSA and decoded, and supplied to the computing unit RE to be compared with the identification number and the count of the infrared signal. In case of agreement the ignition coil ZD, the starter AN and the fuel pump KP are made ready for operation so that the motor vehicle KFZ may be started.

Thus, five encoded radio signals are on stock in the memory MEMO, by means of which the motor vehicle KFZ may be started five times without having to receive radio signals from the centre ZE in advance. This, for example, is necessary for starting the motor vehicle KFZ at places like underground parkings, where no radio signals can be received. After five starts of the motor vehicle KFZ and without any further radio signals from the centre ZE, another start of the vehicle is impossible. Hence, in case of an unallowed use of the motor vehicle KFZ the number of starts of the vehicle may be limited by suppressing the transfer of radio signals from the centre ZE to the motor vehicle KFZ. This suppression of the transfer of radio signals is for example possible by erasion of the individual identification number of the motor vehicle KFZ in the database of the centre ZE.

Fig. 4 shows a schematic diagram of the centre ZE of Fig. 1

The centre ZE incorporates a transmitting equipment SEN, a receiving equipment, a control unit UNIT having a comparator VER and a database DB.

The request signals of the security device SE are received via the receiving equipment EMP. The request signals are supplied to the comparator VER, which detects if the identification number in the respective request signal agrees with with a number stored in the database DB. Only in case of agreement the respective request signal is transferred. It is also possible to erase individual identification numbers in the database DB via the comparator VER, in order to present a transfer of the request signals and to suppress a transmission of the radio signals for individual motor vehicles.

The control unit UNIT comprises an exclusive-OR-gate XOR, an RSA encoding unit RSA, a read-only memory KEY1 for storing a secret key, and a generator GEN. The transferred request signals are supplied to the RSA-encoding unit RSA and to the generator GEN.

The exclusive-OR-gate XOR has two inputs and one output. The request signals are encoded in the RSA-encoding unit and are supplied five times to the first input of the exclusive-OR-gate XOR. Further, the request signals are supplied to the generator GEN. In the generator GEN five signals are generated which are sequentially supplied to the second input of the exclusive-OR-gate XOR. The first of the five signals comprises the count contained in the request signals. The second signal comprises the count increased by one unit. The third, fourth and fifth signals correspondingly contain the count increased by two, three and four units. The signals applied to the output of the exclusive-OR-gate XOR are supplied to the transmitting equipment SEN for transmission to the security device SE of the motor vehicle KFZ.

.....

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 21 902 A 1**

(51) Int. Cl.[6]:
B 60 R 25/00
B 60 R 25/04

(21) Aktenzeichen: 195 21 902.3
(22) Anmeldetag: 16. 6. 95
(43) Offenlegungstag: 19. 12. 96

(1)

DE 195 21 902 A 1

(71) Anmelder:
Alcatel SEL AG, 70435 Stuttgart, DE

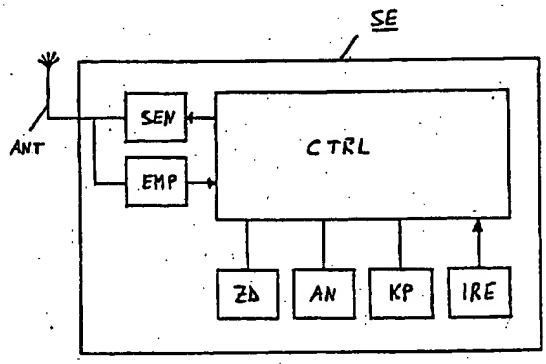
(72) Erfinder:
Beier, Wolfgang, Dipl.-Ing., 71263 Weil der Stadt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 44 15 019 C1
DE 44 15 059 A1
DE 44 15 052 A1
DE 44 05 385 A1
DE 44 03 873 A1
DE 43 20 174 A1
DE 43 00 600 A1

(54) Sicherungseinrichtung für Kraftfahrzeuge

(57) Eine Sicherungseinrichtung (SE) für Kraftfahrzeuge (KFZ), eine sog. Wegfahrsperre, dient zum Sichern des jeweiligen Kraftfahrzeugs (KFZ) gegen unerlaubte Benutzung. Die Sicherungseinrichtung (SE) wird z. B. über den Zündschlüssel (ZD) mit integriertem Infrarot-Sender (IRS) betätigt. Gelangt der Zündschlüssel (ZS) in die Hände eines Diebes, ist die Sicherungseinrichtung (SE) unwirksam. Die Erfindung betrifft eine Sicherungseinrichtung (SE), die über Funksignale, z. B. GSM-Signale betätigbar ist. Die Sicherungseinrichtung (SE) beinhaltet dazu eine Steuereinrichtung (CTRL), eine Empfangseinrichtung (EMP) und wenigstens ein Mittel (AN, ZD, KP), das für die Inbetriebnahme des Kraftfahrzeugs (KFZ) erforderlich ist. Von einer Zentrale (ZE) aus werden für jedes Kraftfahrzeug (KFZ) individuelle Funksignale, z. B. in festen Zeitabständen oder auf Anforderung durch das jeweilige Kraftfahrzeug (KFZ), ausgesendet, die in der Empfangseinrichtung (EMP) empfangen und der Steuereinrichtung (CTRL) zugeführt werden. Die Steuereinrichtung (CTRL) steuert das wenigstens eine Mittel (AN, ZD, KP) in Abhängigkeit von den empfangenen Funksignalen derart an, daß es betriebsbereit oder blockiert ist.



DE 195 21 902 A 1

Beschreibung

Die Erfindung betrifft ein Sicherungssystem für Kraftfahrzeuge, eine Sicherungseinrichtung für Kraftfahrzeuge, eine Zentrale zum Fernsteuern von Kraftfahrzeugen und ein Verfahren zum Fernsteuern von Kraftfahrzeugen.

Sicherungseinrichtungen für Kraftfahrzeuge, sog. Wegfahrsperren, dienen dem elektronischen Sichern von Kraftfahrzeugen gegen unerlaubte Benutzung. Sie blockieren z. B. den Anlasser und die Kraftstoffpumpe und verhindern somit eine Inbetriebnahme der Kraftfahrzeuge. Eine Sicherungseinrichtung wird z. B. über Infrarotsignale über einen Zündschlüssel mit integriertem Infrarot-Sender betätigt. Gelangt der Zündschlüssel in die Hände eines Diebes, ist die Sicherungseinrichtung unwirksam.

Eine Möglichkeit, Kraftfahrzeuge selbst bei Diebstahl oder Verlust eines Zündschlüssels gegen unerlaubte Benutzung zu sichern, ist aus DE 43 26 514 A1 bekannt. Es ist ein elektronisches Fahrzeug-Diebstahl-Sicherungssystem mit einer Steuereinheit, einer numerischen Tastatur und einem Hauptbremszylinder beschrieben. In Abhängigkeit von der Eingabe einer Persönlichen Identifikations-Nummer über die numerische Tastatur, werden über die Steuereinheit die Bremsen des Fahrzeugs blockiert. Die Eingabe der Persönlichen Identifikations-Nummer hat nach festgelegten Fahrzeit- oder Fahrstreckenintervallen zu erfolgen. Dies ist bedienerunfreundlich. Ein weitere Nachteil ist, daß die numerische Tastatur relativ voluminös ist und im Fahrzeug zugänglich angeordnet werden muß. Des weiteren ist ein Verkehrsgefährdung z. B. bei Stillstand des Fahrzeugs auf einer Kreuzung oder einem Bahngleis nicht auszuschließen.

Eine weitere Möglichkeit, Kraftfahrzeuge selbst bei Diebstahl oder Verlust eines Zündschlüssels gegen unerlaubte Benutzung zu sichern, ist aus dem Artikel "Satellitenhilfe gegen Auto-Klau" in der Zeitschrift Funkschau 16/1993, Seiten 42 bis 45 bekannt. Danach kann bei gestohlenen Kraftfahrzeugen über Satellit von einer Zentrale aus die Benzinpumpe abgestellt werden. Ein Nachteil ist, daß, wenn das Kraftfahrzeug nicht empfangsbereit ist, die Benzinpumpe nicht abgestellt werden kann und das Kraftfahrzeug damit dem Dieb uneingeschränkt zur Verfügung steht.

Es ist deshalb Aufgabe der Erfindung, Kraftfahrzeuge unabhängig von den den berechtigten Personen zugänglichen Mitteln gegen unerlaubte Benutzung zu sichern.

Diese Aufgabe wird durch die Lehre der unabhängigen Patentansprüche 1, 9 und 12 gelöst.

Vorteilhafte Ausgestaltungen sind den abhängigen Patentansprüchen zu entnehmen.

Ein besonderer Vorteil der Erfindung liegt in der Möglichkeit der telemetrischen Überwachung von Kraftfahrzeugen.

Ein weiterer Vorteil ist die hohe Abhörsicherheit der übertragenen Funksignale aufgrund der Verwendung der asymmetrischen Verschlüsselung.

Des weiteren kann die Inbetriebnahme der Kraftfahrzeuge schneller erfolgen, da keine Eingaben erforderlich sind.

Im folgenden wird die Erfindung anhand zweier Ausführungsbeispiele unter Zuhilfenahme der Fig. 1 bis 5 erläutert. Es zeigen:

Fig. 1 eine schematische Darstellung eines ersten Ausführungsbeispiels des erfindungsgemäßen Sicherungssystem für Kraftfahrzeuge,

Fig. 2 einen schematisch dargestellten Aufbau einer erfindungsgemäßen Sicherungseinrichtung für das Sicherungssystem aus Fig. 1,

Fig. 3 eine schematische Darstellung einer Steuereinrichtung für die erfindungsgemäße Sicherungseinrichtung aus Fig. 2,

Fig. 4 eine schematisch dargestellten Aufbau einer erfindungsgemäßen Zentrale für das Sicherungssystem aus Fig. 1 und

Fig. 5 eine schematische Darstellung eines zweiten Ausführungsbeispiels des erfindungsgemäßen Sicherungssystems für Kraftfahrzeuge.

Ein erstes Ausführungsbeispiel der Erfindung wird nun anhand der Fig. 1 bis 4 beschrieben.

Fig. 1 zeigt ein erstes Ausführungsbeispiel eines erfindungsgemäßen Sicherungssystems SYS mit einem Funksystem FS, einem Kraftfahrzeug KFZ und einem Zündschlüssel ZS. Das Sicherungssystem SYS dient dazu, Kraftfahrzeuge KFZ von einer Zentrale ZE aus über Funk gegen unerlaubte Benutzung zu sichern. Zur Erläuterung der Erfindung ist lediglich die Sicherung eines Kraftfahrzeuges in einer Funkzelle des Funksystems FS beschrieben. Für die Sicherung mehrerer Kraftfahrzeuge in mehreren Funkzellen gilt entsprechendes.

Das Kraftfahrzeug KFZ, z. B. ein Personenkraftwagen oder ein Lastkraftwagen, beinhaltet eine Sicherungseinrichtung SE mit einer Antenne, über die die Sicherungseinrichtung SE mit der Zentrale ZE kommunizieren kann. Die Antenne ist z. B. die Antenne einer GSM-Mobilstation, die in der Sicherungseinrichtung enthalten sein kann.

Das Funksystem FS ist als zellulares Mobilfunksystem nach dem GSM-Standard ausgelegt; GSM steht für Global System for Mobile Communication. Ein solches zellulares Mobilfunksystem ist z. B. aus dem Buch "The GSM System for Mobile Communications", 1992, M. Mouly and M. Pautet, Int. Standard Book Number 2-9507190-0-7, Seiten 94 bis 98 und 309 bis 312, bekannt. Das Funksystem FS beinhaltet eine Funkfeststation BTS, eine Funkfeststationssteuerung BSC, eine Funkvermittlungsstelle MSC und die Zentrale ZE. Die Funkfeststation BTS ist über die Funkfeststationssteuerung BSC und die Funkvermittlungsstelle MSC mit der Zentrale ZE verbunden.

Der Zündschlüssel ZS enthält eine Infrarot-Sendeeinheit IRS, eine Zähleinrichtung N und einen per Fingerdruck betätigbaren Schalter S. Die Infrarot-Sendeeinheit IRS dient zum Senden von Infrarotsignalen zur Sicherungseinrichtung SE im Kraftfahrzeug KFZ. Die Zähleinrichtung N ist eine Einrichtung zum Generieren von binären Bitfolgen fester Länge, die über die Infrarot-Sendeeinheit IRS zur Sicherungseinrichtung SE übertragen werden und deren Wertigkeit sich bei jeder Übertragung ändert. Die Zähleinrichtung N wird über den Schalter S gesteuert. Bei jedem Betätigen des Schalters S wird der Zählerstand in der Zähleinrichtung N um eine Einheit erhöht und über die Infrarot-Sendeeinheit IRS ausgesendet.

Fig. 2 zeigt nun einen schematisch dargestellten Aufbau der Sicherungseinrichtung SE aus Fig. 1.

Die Sicherungseinrichtung SE beinhaltet drei Mittel AN, ZD, KP, die für die Inbetriebnahme des Kraftfahrzeugs KFZ erforderlich sind, einen Anlasser AN, eine Zündspule ZD und eine Kraftstoffpumpe KP; jeweils mit elektronischer Steuerung. Die Sicherungseinrichtung SE dient dazu, die drei Mittel AN, ZD, KP auf elektronischem Wege betriebsbereit zu machen oder zu

blockieren. Zu diesem Zweck beinhaltet die Sicherungseinrichtung SE ein Steuereinrichtung CTRL, eine Infrarot-Empfangseinheit IRE, eine Sendeeinrichtung SEN, eine Empfangseinrichtung EMP und eine Antenne ANT. Die Steuereinrichtung CTRL steuert die drei Mittel AN, ZD, KP in Abhängigkeit von den über die Infrarot-Empfangseinheit IRE und über die Empfangseinrichtung EMP empfangenen Signale. Die Steuereinrichtung CTRL ist dazu mit den drei Mitteln AN, ZD, KP, der Infrarot-Empfangseinheit IRE, der Sendeeinrichtung SEN und der Empfangseinrichtung EMP verbunden. Die Sendeeinrichtung SEN und die Empfangseinrichtung EMP sind mit der Antenne ANT verbunden.

Fig. 3 zeigt nun eine schematische Darstellung der Steuereinrichtung CTRL aus Fig. 2.

Die Steuereinrichtung CTRL beinhaltet eine Recheneinheit RE, z. B. einen Mikroprozessor, mit zwei Eingängen und drei Ausgängen. Der erste Ausgang ist mit der Zündspule ZD, der zweite Ausgang mit dem Anlasser AN und der dritte Ausgang mit der Kraftstoffpumpe KP verbunden. In Abhängigkeit von den an den beiden Eingängen der Recheneinheit RE anliegenden Signale, werden die Zündspule ZD, der An lasse AN und die Kraftstoffpumpe KP betriebsbereit gemacht, indem z. B. die Spannungsversorgung für die Zündspule ZD, den Anlasser AN und die Kraftstoffpumpe KP jeweils über ein Relais zugeschaltet wird. Nach jedem Abschalten des Motors werden die Zündspule ZD, der Anlasser AN und die Kraftstoffpumpe KP durch die Recheneinheit RE blockiert, indem z. B. jeweils die Spannungsversorgung über ein Relais abgeschaltet wird. Dazu wird z. B. von der Motorsteuerung ein Steuersignal zur Recheneinheit RE übertragen, sobald der Motor abgestellt wird. Eine erneute Inbetriebnahme des Kraftfahrzeugs KFZ ist nur über neue Eingangssignale für die Recheneinheit RE möglich. Die neuen Eingangssignale müssen sich von den Eingangssignalen der vorherigen Inbetriebnahme unterscheiden. Ein erstes Eingangssignal für die Steuereinrichtung CTRL wird aus dem Infrarot-Signal vom Zündschlüssel ZS gewonnen, ein zweites Eingangssignal aus dem Funksignal von der Zentrale ZE. Sind die beiden Eingangssignale gleich, so werden die Zündspule ZD, der Anlasser AN und die Kraftstoffpumpe KP betriebsbereit gemacht.

Die Steuereinrichtung CTRL enthält des weiteren einen Vergleicher VER, eine Aktualisierungseinheit AKT, einen Speicher MEMO, eine Einleseeinheit IN, eine Ausleseeinheit OUT und eine Identifizierungseinheit ID. Das Infrarotsignal des Zündschlüssels ZS wird zunächst dem Vergleicher VER zugeführt. Im Vergleicher VER findet ein Vergleich zwischen dem im Infrarotsignal enthaltenen Zählerstand und einem in der Aktualisierungseinheit AKT gespeicherten Zählerstand statt. Ist der Zählerstand des Infrarotsignals wenigstens um eine Einheit und maximal um zehn Einheiten höher als der Zählerstand der Aktualisierungseinheit AKT, so wird das Infrarotsignal weitergeschaltet und der Zählerstand in der Aktualisierungseinheit AKT durch den Zählerstand des Infrarotsignals ersetzt. Das Infrarotsignal wird nach Durchlaufen des Vergleichers VER der Identifizierungseinheit ID zugeführt. In der Identifizierungseinheit ID wird dem Zählerstand des Infrarotsignals eine für das Kraftfahrzeug KFZ individuelle Identifizierungs-Nummer zugefügt. Der Zählerstand und die Identifizierungs-Nummer dienen zum einen als erstes Eingangssignal für die Recheneinheit RE und bilden zum anderen ein Anforderungssignal, das über die Sendeeinrichtung SEN der Sicherungseinrichtung SE über Funk zur Zentrale ZE übertragen wird.

Die Zentrale ZE wertet das Anforderungssignal aus, überprüft, ob die Identifizierungs-Nummer in einer Datenbank vorhanden ist, und sendet, falls die Identifizierungs-Nummer in der Datenbank vorhanden ist, fünf verschlüsselte Funksignale zur Steuereinrichtung. Die fünf verschlüsselten Funksignale werden über die Einleseeinheit IN in den Speicher MEMO eingelesen und abgespeichert. Das erste verschlüsselte Funksignal enthält in verschlüsselter Form den Zählerstand des Infrarotsignals und die Identifizierungs-Nummer und wird unter der Speicheradresse abgespeichert, die dem Wert des Zählerstand des Infrarotsignals entspricht. Das zweite verschlüsselte Funksignal enthält den Zählerstand um eine Einheit erhöht und die Identifizierungs-Nummer und wird unter der Speicheradresse mit dem Wert des um eine Einheit erhöhten Zählerstand abgespeichert. Vergleichbares gilt für das dritte, vierte und fünfte Funksignal.

Die Steuereinrichtung CTRL enthält des weiteren ein Exklusiv-ODER-Gatter XOR, eine RSA-Entschlüsselungseinheit RSA und einen Nur-Lese-Speicher KEY2, in dem ein öffentlicher Schlüssel gespeichert ist. RSA steht für Rivest, Shamir, Adleman. Nach RSA können Signale asymmetrisch verschlüsselt und entschlüsselt werden. Die Verschlüsselungsmethode nach RSA ist z. B. aus dem Buch "Chipkarten-Technologie in der Anwendung", 1995, Seiten 47 bis 54, Wissenschaftsverlag Volker Spiess GmbH, Berlin, ISBN 3-89166-183-5 bekannt.

Die Zentrale ZE verschlüsselt Signale mit einem geheimen Schlüssel nach dem RSA-Algorithmus. Der geheime Schlüssel ist z. B. 512 bit lang und nur der Zentrale ZE bekannt. Die Steuereinichtung CTRL im Kraftfahrzeug KFZ hat zur Entschlüsselung nach dem RSA-Algorithmus einen öffentlichen Schlüssel, der für mehrere Kraftfahrzeuge KFZ verwendet werden kann und auch der Öffentlichkeit bekannt sein kann.

Das Exklusiv-ODER-Gatter XOR hat zwei Eingänge und eine Ausgang. Der Ausgang ist über die RSA-Entschlüsselungseinheit RSA mit dem zweiten Eingang der Recheneinheit verbunden. An den ersten Eingang wird der Zählerstand des Infrarotsignals angelegt. An den zweiten Eingang wird der Speicherinhalt angelegt, der zur Speicheradresse zugehörig ist, die dem Zählerstand des Infrarotsignals entspricht. Der Speicherinhalt wird somit mit dem Zählerstand des Infrarotsignals verknüpft, der RSA-Entschlüsselungseinheit RSA zugeführt, dort entschlüsselt und der Recheneinheit RE zwecks Vergleich mit der Identifizierungs-Nummer und dem Zählerstand des Infrarotsignals zugeführt. Bei Übereinstimmung werden die Zündspule ZD, der Anlasser AN und die Kraftstoffpumpe KP betriebsbereit gemacht, so daß das Kraftfahrzeug KFZ in Betrieb genommen werden kann.

In dem Speicher MEMO sind somit fünf verschlüsselte Funksignale auf Vorrat gespeichert, mit denen das Kraftfahrzeug KFZ fünfmal in Betrieb genommen werden kann, ohne daß das Kraftfahrzeug KFZ vorher Funksignale von der Zentrale ZE zu empfangen braucht. Dies ist z. B. für Inbetriebnahmen des Kraftfahrzeugs KFZ erforderlich an Orten, z. B. Tiefgaragen, wo keine Funksignale empfangen werden können. Nach fünf Inbetriebnahmen des Kraftfahrzeugs KFZ und ohne weitere Funksignale von der Zentral ZE ist ein erneute Inbetriebnahme des Kraftfahrzeugs KFZ nicht möglich. Bei unerlaubter Benutzung des Kraftfahrzeugs KFZ ist somit durch Unterdrückung der Übertragung

von Funksignalen von der Zentrale ZE zum Kraftfahrzeug KFZ die Anzahl der Inbetriebnahmen des Kraftfahrzeugs KFZ limitierbar. Die Unterdrückung der Übertragung von Funksignalen ist z. B. durch die Löschung der für jedes Kraftfahrzeug KFZ individuellen Identifizierungs-Nummer in der Datenbank der Zentrale ZE möglich.

Fig. 4 zeigt nun einen schematisch dargestellten Aufbau der Zentrale ZE aus Fig. 1.

Die Zentrale ZE beinhaltet eine Sendeeinrichtung SEN, eine Empfangseinrichtung, eine Steuereinheit UNIT mit einem Vergleicher VER und eine Datenbank DB.

Über die Empfangseinrichtung EMP werden die Anforderungssignale der Sicherungseinrichtung SE empfangen. Die Anforderungssignale werden dem Vergleicher VER zugeführt, in dem ermittelt wird, ob die Identifizierungs-Nummer im jeweiligen Anforderungssignal mit einer in der Datenbank DB gespeicherten Nummer übereinstimmt. Nur die Übereinstimmung wird das jeweiligen Anforderungssignal weitergeleitet. Über den Vergleicher VER können auch einzelne Identifizierungs-Nummern in der Datenbank DB gelöscht werden, um eine Weiterleitung der Anforderungssignale zu verhindern und eine Übertragung von Funksignalen für einzelne Kraftfahrzeuge zu unterdrücken.

Die Steuereinheit UNIT beinhaltet ein Exklusiv-ODER-Gatter XOR, eine RSA-Verschlüsselungseinheit RSA, einen Nur-Lese-Speicher KEY1 zum Speichern eines geheimen Schlüssels und einen Generator GEN. Die weitergeleiteten Anforderungssignale werden der RSA-Verschlüsselungseinheit RSA und dem Generator GEN zugeführt.

Das Exklusiv-ODER-Gatter XOR hat zwei Eingänge und einen Ausgang. Die Anforderungssignale werden in der RSA-Verschlüsselungseinheit RSA verschlüsselt und dem ersten Eingang des Exklusiv-ODER-Gatters XOR fünfmal zugeführt. Die Anforderungssignale werden des weiteren dem Generator GEN zugeführt. Im Generator GEN werden fünf Signale generiert, die sequentiell dem zweiten Eingang des Exklusiv-ODER-Gatters XOR zugeführt werden. Das erste der fünf Signale beinhaltet den in den Anforderungssignalen enthaltenen Zählerstand. Das zweite Signal beinhaltet den um eine Einheit erhöhten Zählerstand. Das dritte, vierte und fünfte Signal beinhaltet entsprechend den um zwei, drei und vier Einheiten erhöhten Zählerstand. Die am Ausgang des Exklusiv-ODER-Gatters XOR anliegenden Signale werden der Sendeeinrichtung SEN zur Übertragung zur Sicherungseinrichtung SE des Kraftfahrzeugs KFZ zugeführt.

Ein zweites Ausführungsbeispiel der Erfindung wird nun anhand der Fig. 5 beschrieben.

Fig. 5 zeigt ein zweites Ausführungsbeispiel des erfindungsgemäßen Sicherungssystems SYS mit einer Zentrale ZE und einer in einem Kraftfahrzeug angeordneten Sicherungseinrichtung SE. Das Sicherungssystem SYS dient dazu, Kraftfahrzeuge von der Zentrale ZE aus über Funk gegen unerlaubte Benutzung zu sichern. Die Zentrale ZE beinhaltet zu diesem Zweck eine Sendeeinrichtung SEN, eine Steuereinheit UNIT und eine Datenbank DB. Die Datenbank DB ist z. B. ein EEPROM oder ein RAM-Speicher. In der Datenbank DB sind mehrere Blöcke gespeichert. Jeder Block enthält eine für jedes Kraftfahrzeug individuelle Identifizierungs-Nummer ID und n Kodes CODE1, CODE2, .., CODEn, die für jedes Kraftfahrzeug unterschiedliche Inhalte haben können; n ist eine natürliche Zahl, z. B. 365. Bei m Kraftfahrzeugen erhält man somit m Identifizierungs-Nummer ID1 bis IDm; m ist z. B. 100 000.

Die Steuereinheit UNIT beinhaltet eine Mikroprozessor und eine Ringzähler. Der Ringzähler zählt fortlaufend in Einer-Schritten von 1 bis n und beginnt wieder bei 1, wenn er den Zählerstand n erreicht hat. Jedem Zählerstand ist in jedem Block ein Kode zugeordnet. Jeder Einer-Schritt wird z. B. alle 24 Stunden einmal durchgeführt. Zu jedem Zählerstand des Ringzählers wird, gesteuert durch den Mikroprozessor, für jedes Kraftfahrzeug ein Signal erzeugt, daß die Identifizierungs-Nummer ID des Kraftfahrzeugs und den aktuellen Kode CODE1, CODE2, .., CODEn enthält, der dem aktuellen Zählerstand des Ringszählers zugehörig ist. Die Signale mit den Identifizierungs-Nummern ID1 bis IDm werden z. B. alle acht Stunden zur Sendeeinrichtung SEN übertragen, in der sie zu Funksignalen aufbereitet werden. Die Sendeeinrichtung ist mit einer Antenne ANT verbunden. Die Antenne ANT ist z. B. die Antenne einer Rundfunkstation. Die Funksignale können z. B. über Ultrakurzwelle mit dem RDS-System übertragen werden. RDS steht für Radio-Daten-System und ist z. B. aus dem Buch "Taschenbuch der Nachrichtentechnik", 1988, Seiten 163 und 164, Fachverlag Schiele und Schön, ISBN 3-7949-0477-X bekannt. Um eine Erreichbarkeit in größeren Gebieten, z. B. für Europa sicherzustellen, kann als Rundfunkstation z. B. diejenige des Senders "Deutsche Welle" in Köln verwendet werden. Die Funksignale werden dann z. B. bei einer Frequenz von 6,075 kHz oder 15,145 kHz übertragen.

Die Sicherungseinrichtung SE beinhaltet eine Empfangseinrichtung EMP, eine Steuereinrichtung CTRL, eine Zündspule ZD, einen Anlasser AN und eine Kraftstoffpumpe KP.

Die Empfangseinrichtung EMP ist mit einer Antenne AT verbunden. Die Antenne AT ist z. B. die Antenne eines Autoradios. Über die Empfangseinrichtung können die von der Zentrale ZE gesendeten Funksignale empfangen, ausgewertet und der Steuereinrichtung CTRL zugeführt werden. Die Empfangseinrichtung EMP beinhaltet dazu einen Vergleicher in dem festgestellt wird, ob in dem empfangenen Funksignal die für das Kraftfahrzeug individuelle Identifizierungs-Nummer ID enthalten ist. Falls dies der Fall ist, ist das Funksignal für das Kraftfahrzeug bestimmt und der in den Funksignalen enthaltene aktuelle Kode CODE wird zur Steuereinrichtung CTRL übertragen. Zur Initialisierung wird von der Zentrale ZE anstelle des aktuellen Kodes CODE der aktuelle Zählerstand des Ringzählers gesendet.

Die Steuereinrichtung CTRL beinhaltet eine Recheneinheit RE, einen Speicher MEMO und ein Ausleseeinheit OUT. Die Ausleseeinheit OUT enthält einen Ringzähler, der bei der Initialisierung durch die Übertragung des aktuellen Zählerstandes des Ringzählers der Zentrale ZE auf diesen synchronisiert wird.

Der Speicher MEMO ist z. B. ein Nur-Lese-Speicher. Im Speicher sind n Kodes CODE1, CODE2, .., CODEn gespeichert, n ist z. B. 365. Die n Kodes CODE1, CODE2, .., CODEn entsprechen denjenigen in der Datenbank DB der Zentrale ZE für das jeweilige Kraftfahrzeug in einem Block abgespeicherten n Kodes. Auch die Zuordnung der Zählerstände des Ringzählers zu den n Kodes ist in der jeweiligen Sicherungseinrichtung SE und in der Zentrale ZE identisch.

Die Recheneinheit RE hat zwei Eingänge und drei Ausgänge, einen Vergleicher, zwei Zähler und eine Steuerung, z. B. einen Mikroprozessor, die den Vergleicher und die beiden Zähler steuert und deren Ausgangs-

signale auswertet. Der erste Ausgang ist mit der Zündspule ZD, der zweite mit dem Anlasser und der dritte mit der Kraftstoffpumpe KP verbunden. Die Recheneinheit RE dient dazu, die Zündspule ZD, den Anlasser AN und die Kraftstoffpumpe KP zu blockieren oder betriebsbereit zu machen. Die Zündspule ZD, der Anlasser AN und die Kraftstoffpumpe KP werden durch die Recheneinheit RE blockiert, sobald der Motor abgeschaltet wird und indem z. B. die Spannungsversorgung für die Zündspule ZD, den Anlasser AN und die Kraftstoffpumpe KP jeweils über ein Relais abgeschaltet wird. Eine erneute Inbetriebnahme des Kraftfahrzeugs KFZ ist nur über neue Eingangssignale für die Recheneinheit möglich. Liegen an den beiden Eingängen der Recheneinheit RE die gleichen Signale an, was z. B. über den Vergleicher festgestellt wird, so werden die sich in der Recheneinheit RE befindlichen Zähler auf Null zurückgesetzt und die Zündspule ZD, der Anlasser AN und die Kraftstoffpumpe KP betriebsbereit gemacht. Der Vergleicher vergleicht die beiden Eingangssignale der Recheneinheit RE alle 24 Stunden. Wird bei einem Vergleich festgestellt, daß die beiden Eingangssignale unterschiedlich sind, so wird der Zählerstand des ersten Zählers um Eins erhöht. Erreicht der erste Zähler den Zählerstand Drei, so wird der zweite Zähler aktiviert, der bei jeder weiteren Inbetriebnahme seinen Zählerstand um Eins erhöht. Erreicht der zweite Zähler den Zählerstand Drei, so werden die Zündspule ZD, der Anlasser AN und die Kraftstoffpumpe KP über die Steuerung elektronisch blockiert, so daß eine weitere Inbetriebnahme des Kraftfahrzeugs nicht mehr möglich ist.

Die Funksignale von der Zentrale ZE zum Kraftfahrzeug KFZ werden alle acht Stunden gesendet. Bei einer unerlaubten Benutzung des Kraftfahrzeugs wird die Übertragung von Funksignalen für das jeweilige Kraftfahrzeug unterdrückt, so daß das Kraftfahrzeug nach drei Tagen und drei weiteren Inbetriebnahmen blokkiert ist.

Die von der Zentrale ZE zum Kraftfahrzeug KFZ gesendeten Funksignale sind individuelle Funksignale. Das bedeutet, daß die Zentrale z. B. im Zeitmultiplexverfahren jedem Kraftfahrzeug KFZ die jeweiligen individuellen Funksignale sendet. Die individuellen Funksignale können auch in Rahmen übertragen werden. Die Kraftfahrzeuge KFZ synchronisieren dann auf das Rahmenkennwort und werten jeweils in dem ihnen zugeordneten Zeitschlitz die jeweiligen individuellen Funksignale aus.

Beim ersten Ausführungsbeispiel kann zur Lokalisierung des Kraftfahrzeugs, was bei unerlaubter Benutzung des Kraftfahrzeugs von Vorteil wäre, zusätzlich zum Anforderungssignal ein weiteres in derjenigen Funkfeststation BTS, die das Anforderungssignal empfangen hat, erzeugtes Signal mit der Angabe der Funkzelle zur Zentrale ZE übertragen werden. Des weiteren oder alternativ könnte im jeweiligen Anforderungssignal zusätzlich ein GPS-Signal zur Zentrale ZE übertragen werden. GPS steht für Global Positioning System, ist ein Satellitennavigationssystem und z. B. aus der Zeitschrift "Funkschau", Heft 11/1993, Seiten 74 bis 77 bekannt. Zur Erzeugung des GPS-Signals muß die Sicherungseinrichtung SE zusätzlich einen GPS-Empfänger beinhalten.

In beiden Ausführungsbeispielen sind alle Zahlenangaben, z. B. die Anzahl der in der Datenbank gespeicherten Kodes, die Anzahl der im Speicher gespeicherten verschlüsselten Funksignale oder die Zeitabstände für die Übertragung von Funksignalen von der Zentrale ZE zu den Kraftfahrzeugen beispielhaft.

Beim zweiten Ausführungsbeispiel kann unabhängig von den empfangenen Funksignalen zum Betriebsbereitmachen der Zündspule SD, des Anlassers AN und der Kraftstoffpumpe KP zusätzlich ein weiterer Kode erforderlich sein. Der weitere Kode kann z. B. über ein vom Zündschlüssel gesendetes Infrarotsignal zur Sicherungseinrichtung SE übertragen werden. Die Sicherungseinrichtung SE benötigt dazu eine Infrarot-Empfangseinheit und eine Recheneinheit RE, die die Zündspule ZD, den Anlasser AN und die Kraftstoffpumpe KP erst dann betriebsbereit macht, wenn auch der weitere Kode vorliegt.

Patentansprüche

1. Sicherungseinrichtung (SE) für Kraftfahrzeuge (KFZ) mit einem für die Inbetriebnahme des Kraftfahrzeugs erforderlichen Mittel (AN, ZD, KP), mit einer Empfangseinrichtung (EMP) zum Empfang von Funksignalen und mit einer Steuereinrichtung (CTRL) zum Steuern des Mittels (AN, ZD, KP),
bei der die empfangenen Funksignale über die Empfangseinrichtung (EMP) der Steuereinrichtung zuführbar sind, und
bei der das Kraftfahrzeug (KFZ) nach Empfang von individuellen Funksignalen in Betrieb genommen werden kann.

2. Sicherungseinrichtung (SE) nach Anspruch 1, dadurch gekennzeichnet, daß die Sicherungseinrichtung (SE) eine Sendeeinrichtung (SEN) zum Anfordern der individuellen Funksignale beinhaltet.

3. Sicherungseinrichtung (SE) nach Anspruch 1, dadurch gekennzeichnet, daß die Steuereinrichtung (CTRL) einen Speicher (MEMO) und eine Einleseeinheit (IN) beinhaltet, und daß über die Einleseeinheit (IN) die empfangenen individuellen Funksignale im Speicher (MEMO) abspeicherbar und für mehrere Inbetriebnahmen des Kraftfahrzeugs (KFZ) verwendbar sind.

4. Sicherungseinrichtung (SE) nach Anspruch 1, dadurch gekennzeichnet, daß die Steuereinrichtung (CTRL) eine RSA-Entschlüsselungseinheit (RSA) zum Entschlüsseln der empfangenen Funksignale beinhaltet.

5. Sicherungseinrichtung (SE) nach Anspruch 1, dadurch gekennzeichnet, daß die Sicherungseinrichtung (SE) eine Infrarot-Empfangseinrichtung (IRE) zum Empfang von Infrarotsignalen beinhaltet, und daß nach Empfang von individuellen Funksignalen und von Infrarotsignalen das Kraftfahrzeug (KFZ) in Betrieb genommen werden kann.

6. Sicherungseinrichtung (SE) nach Anspruch 2, dadurch gekennzeichnet, daß die Sicherungseinrichtung (SE) eine Infrarot-Empfangseinheit (IRE) zum Empfang von Infrarotsignalen beinhaltet, daß die Steuereinrichtung (CTRL) eine Recheneinheit (RE) und eine Identifizierungseinheit (ID) beinhaltet, daß die empfangenen Infrarotsignale in der Identifizierungseinheit (ID) verarbeitbar sind, daß die verarbeiteten Infrarotsignale der Sendeeinrichtung (SEN) und der Recheneinheit (RE) zuführbar sind, daß die empfangenen Funksignale der Recheneinheit (RE) zuführbar sind, und daß in Abhängigkeit von den verarbeiteten Infrarotsignalen und in Abhängigkeit von den empfangenen Funksignalen das Kraftfahrzeug (KFZ) in Betrieb genommen werden kann.

7. Sicherungseinrichtung (SE) nach Anspruch 1, dadurch gekennzeichnet, daß die Sicherungseinrichtung (SE) eine GSM-Mobilstation beinhaltet.

8. Sicherungseinrichtung (SE) nach Anspruch 2, dadurch gekennzeichnet, daß die Sicherungseinrichtung (SEC einen GPS-Empfänger beinhaltet, und daß die empfangenen GPS-Signale der Sendeeinrichtung (SEN) zuführbar sind.

9. Zentrale (ZE) zum Fernsteuern von Kraftfahrzeugen (KFZ) mit einer Sendeeinrichtung (SEN) zum Senden von Funksignalen, mit einer Steuereinheit (UNIT) und mit einer Datenbank (DB), bei der in der Datenbank (DB) für jedes Kraftfahrzeug (KFZ) individuelle Daten speicherbar sind und bei der gesteuert durch die Steuereinheit (UNIT) von der Sendeeinrichtung (SEN) aus für jedes Kraftfahrzeug (KFZ), für das in der Datenbank (DB) individuelle Daten gespeichert sind, individuelle Funksignale sendbar sind.

10. Zentrale (ZE) nach Anspruch 9, dadurch gekennzeichnet, daß die Zentrale (ZE) eine Empfangseinrichtung (EMP) zum Empfangen von Funksignalen beinhaltet, daß die Steuereinheit (UNIT) einen Vergleicher (VER) beinhaltet, daß der Vergleicher (VER) mit der Empfangseinrichtung (EMP) und der Datenbank (DB) verbunden ist, daß die empfangenen Funksignale im Vergleicher (VER) mit den in der Datenbank (DB) gespeicherten Daten vergleichbar, und daß die Weiterleitung der empfangenen Funksignale in Abhängigkeit vom Ergebnis des Vergleichs unterdrückbar ist.

11. Zentrale (ZE) nach Anspruch 10, dadurch gekennzeichnet, daß die Steuereinheit (UNIT) eine RSA-Verschlüsselungseinheit (RSA) beinhaltet, daß die weitergeleiteten empfangenen Funksignale in der RSA-Verschlüsselungseinheit (RSA) verschlüsselbar, und daß die verschlüsselten Signale der Sendeeinrichtung (SEN) zuführbar sind.

12. Verfahren zum Fernsteuern von Kraftfahrzeugen (KFZ), bei dem von einer Zentrale (ZE) aus Funksignale zu den Kraftfahrzeugen (KFZ) übertragen werden,
bei dem die Funksignale für jedes Kraftfahrzeug (KFZ) individuelle Daten beinhalten und
bei dem in Abhängigkeit von den übertragenen Funksignalen im jeweiligen Kraftfahrzeug (KFZ) ein für die Inbetriebnahme des Kraftfahrzeugs (KFZ) erforderliches Mittel (AN, ZD, KP), durch eine Steuereinrichtung (CTRL) derart angesteuert wird, daß das Kraftfahrzeug (KFZ) in Betrieb genommen werden kann.

Hierzu 5 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 21 902 A1
Int. Cl.[6]: B 60 R 25/00
Offenlegungstag: 19. Dezember 1996

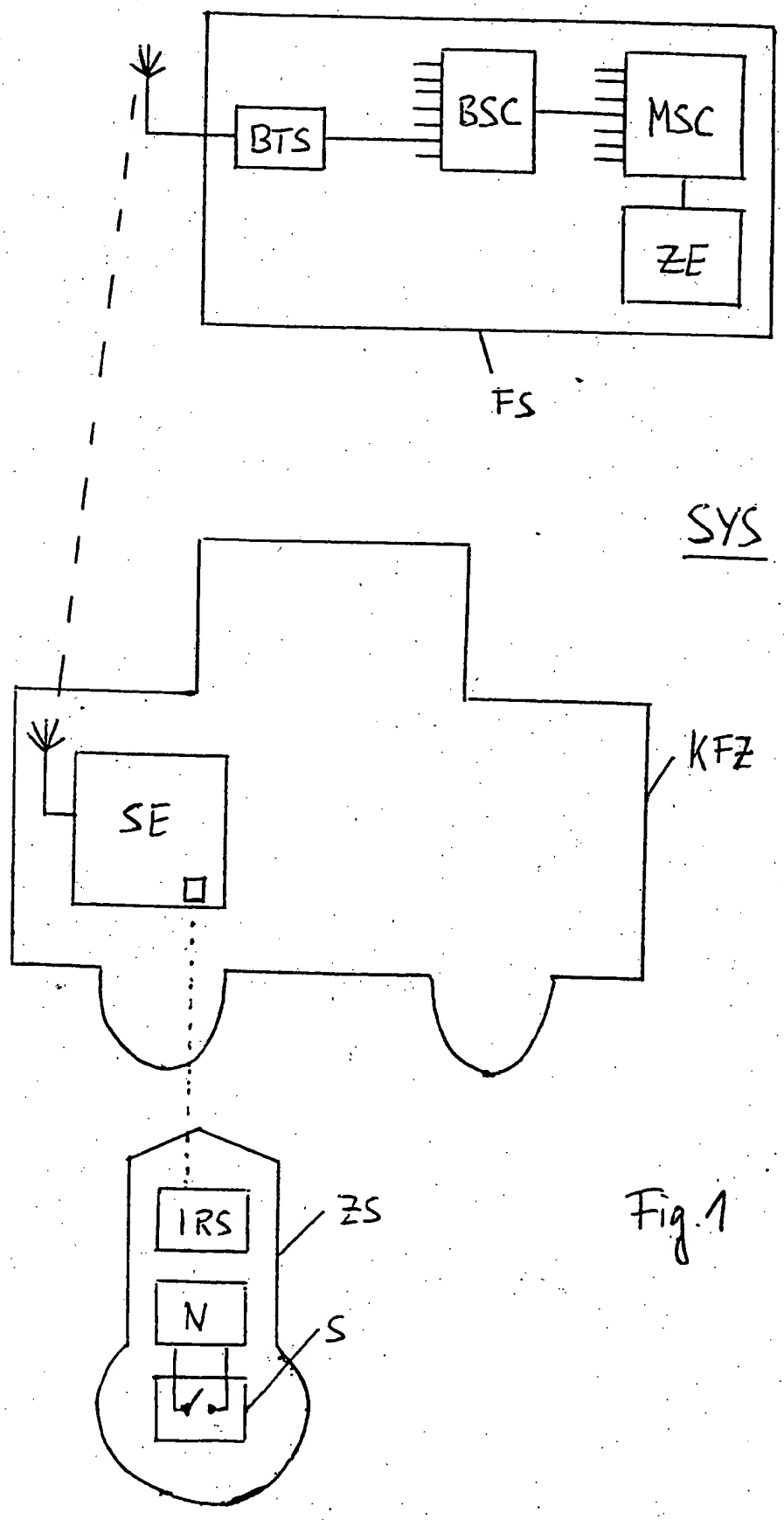


Fig. 1

Nummer: DE 195 21 902 A1
Int. Cl.[6]: B 60 R 25/00
Offenlegungstag: 19. Dezember 1996

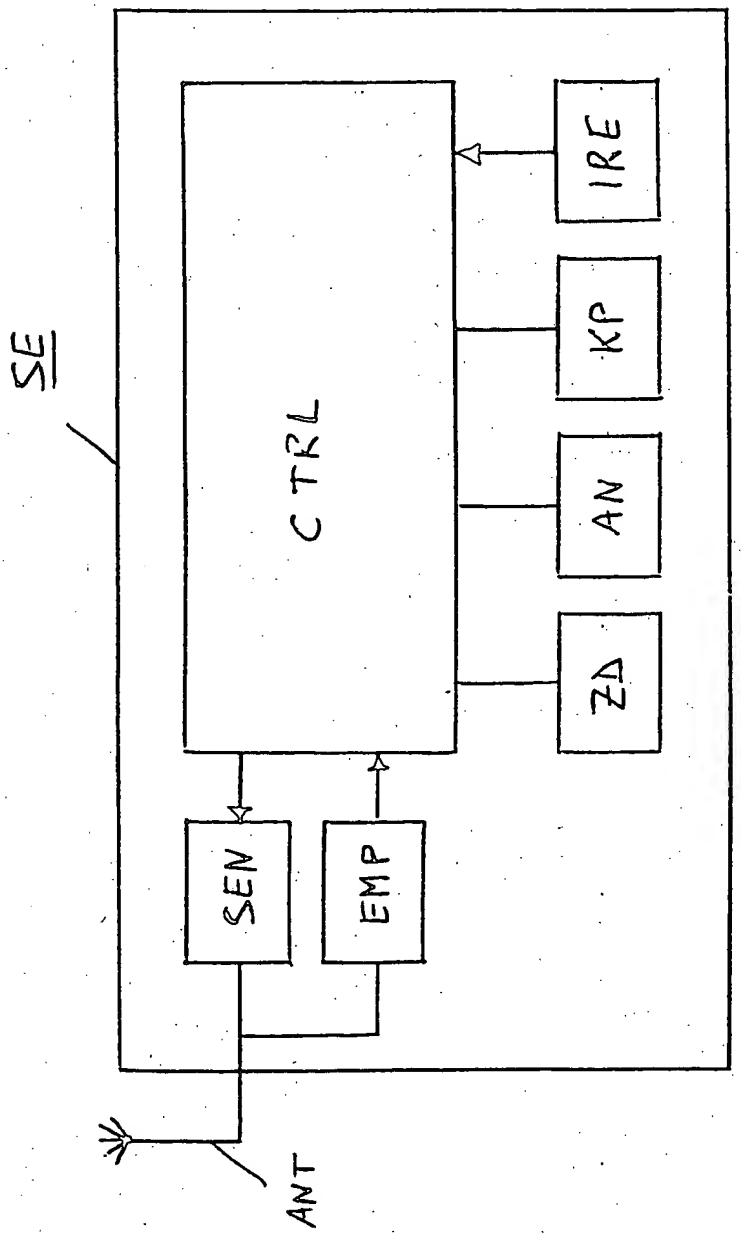


Fig. 2

Nummer: DE 195 21 902 A1
Int. Cl.[6]: B 60 R 25/00
Offenlegungstag: 19. Dezember 1996

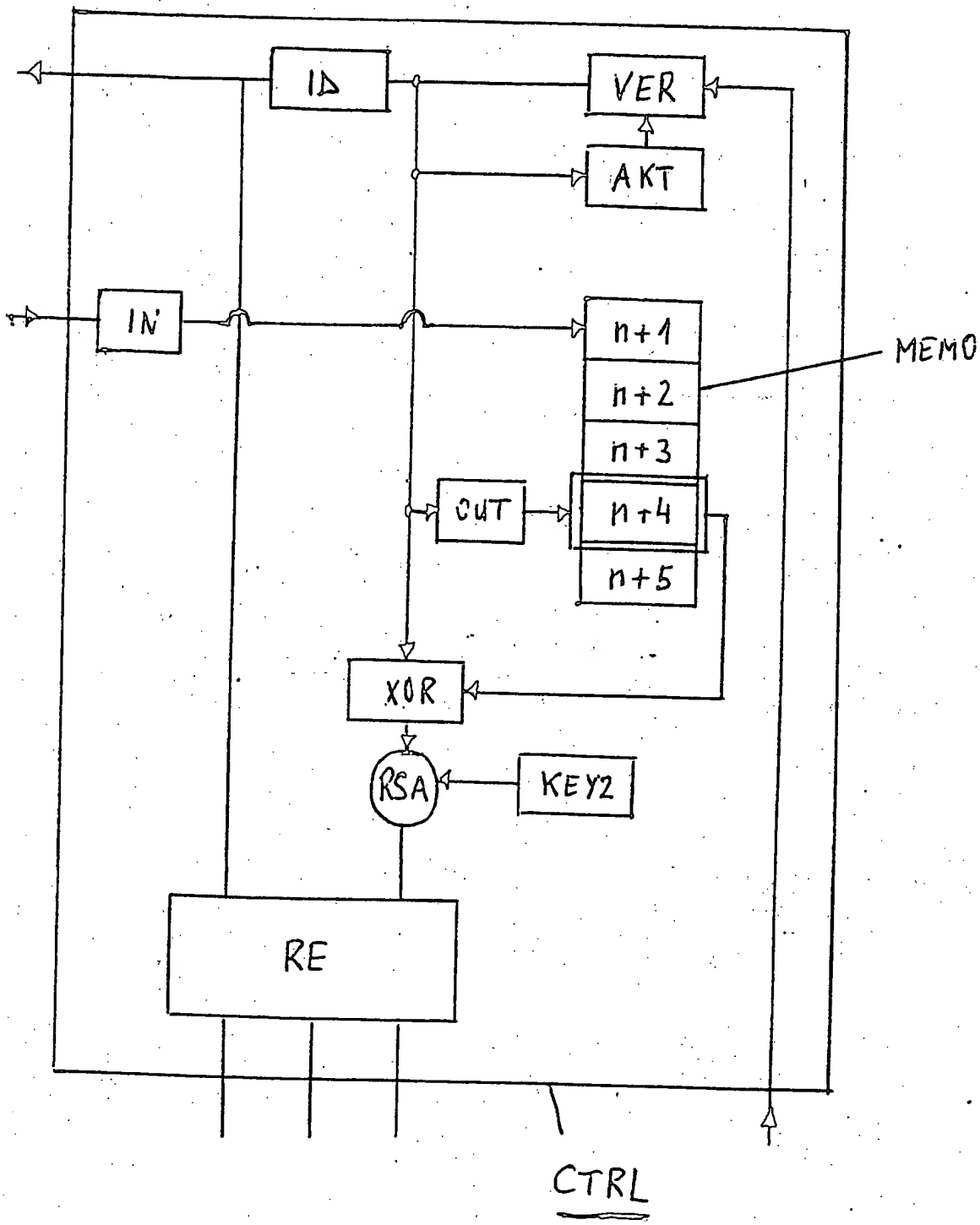


Fig. 3

Nummer: DE 195 21 902 A1
Int. Cl.[6]: B 60 R 25/00
Offenlegungstag: 19. Dezember 1996

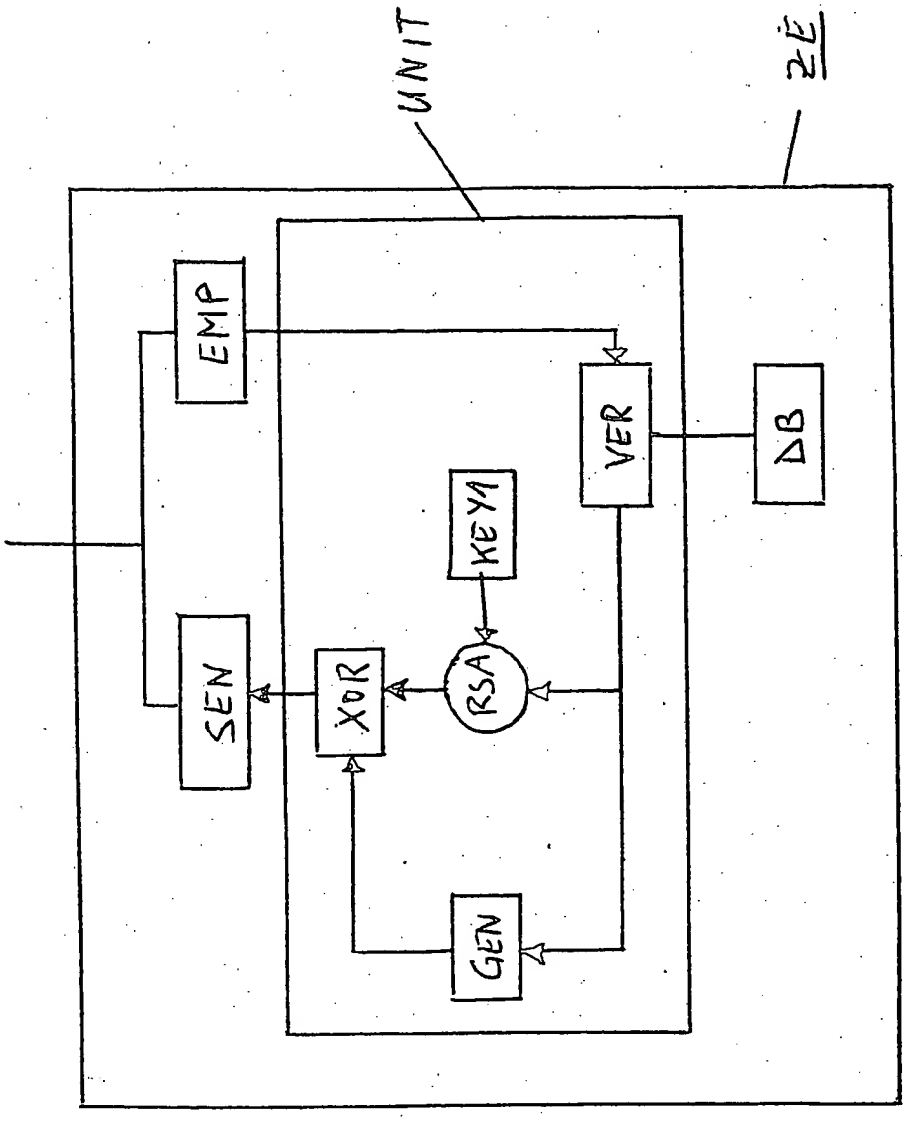


Fig. 4

Nummer: DE 195 21 902 A1
Int. Cl.[6]: B 60 R 25/00
Offenlegungstag: 19. Dezember 1996

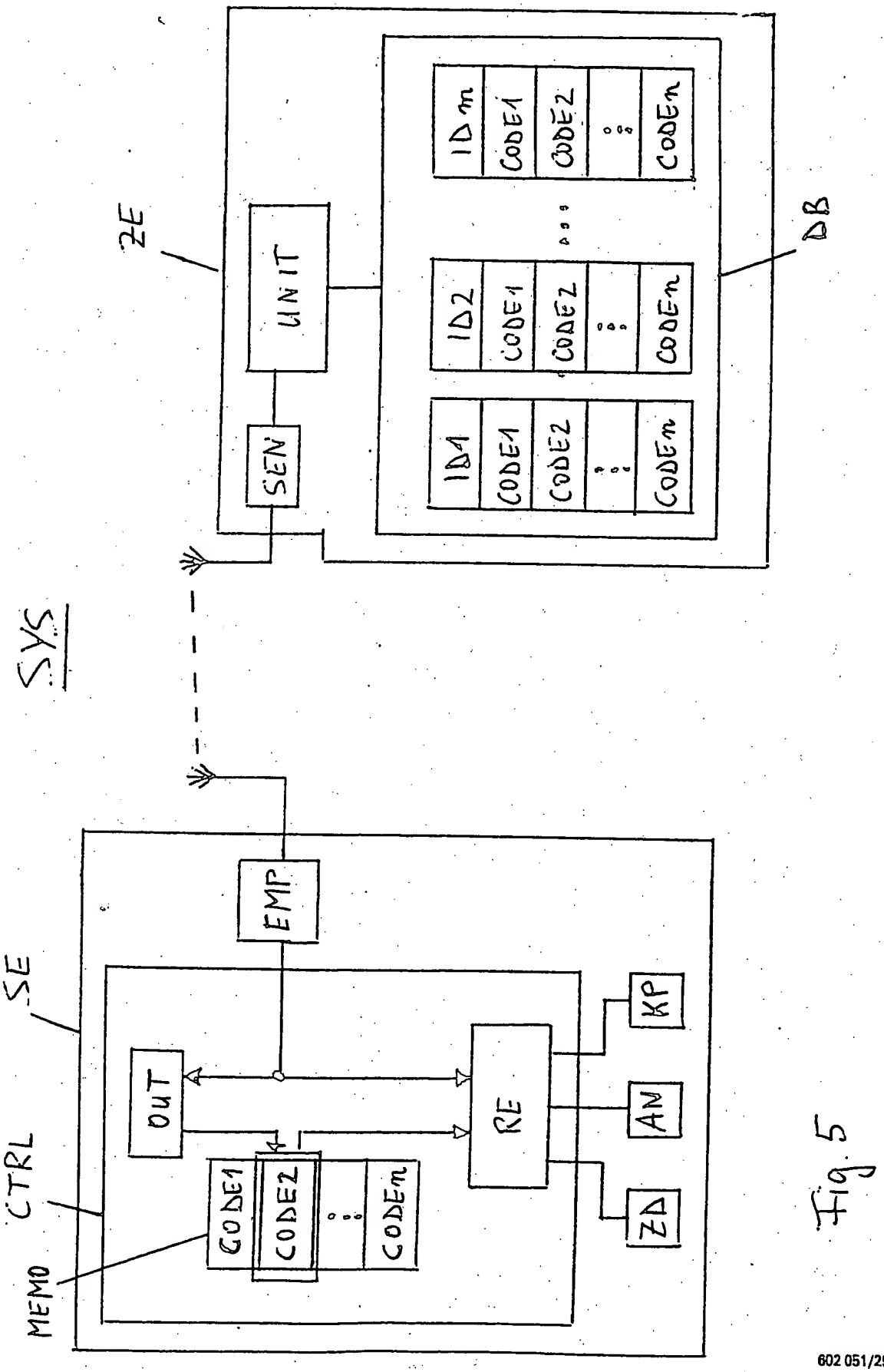


Fig. 5